

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims in accordance with the following:

Please ADD new claims according to the following.

1. (Currently Amended) A security management device including:
a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;
a judging unit judging ~~by comparing whether~~ the security level of the user apparatus ~~reaches~~with a predetermined security level; and
an access control unit, in case the judging unit judges ~~that~~ the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user of the apparatus.
2. (Currently Amended) A security management device according to Claim 1, wherein the access control unit, in case the judging unit judges that the security level of the user apparatus reaches the predetermined level, sets a range wider than the restriction range as the access permission range of the user apparatus.
3. (Currently Amended) A security management device according to Claim 1, wherein the access control unit has a function of ~~selecting~~ controlling a communication route of the user apparatus and, in case the judging unit judges that the security level of the user apparatus does not reach the predetermined level, ~~changes~~ controls a communication destination of the user apparatus to a specified device in the restriction range on the network.
4. (Currently Amended) A security management device according to Claim 3, wherein the specified device controls updating the virus definition file of the user apparatus ~~sets~~

~~the security level of the apparatus or provides a setting guide to the apparatus.~~

5. (CURRENTLY AMENDED) A ~~security management method by which of managing computer security comprising a computer executes the steps of:~~

detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

judging by comparing whether the security level of the user apparatus with reaches a predetermined security level; and

in the case of judging that the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus.

6. (CURRENTLY AMENDED) A security management method according to Claim 5, ~~including a step of, in the~~ wherein in case of judging that the security level of the user apparatus reaches the predetermined level, setting a range wider than the restriction range as the access permission range of the user apparatus.

7. (CURRENTLY AMENDED) A security management method according to Claim 5, wherein in case ~~the step judges that of~~ judging the security level of the user apparatus does not reach the predetermined level, ~~in the step of the~~ restricting of the access permission range of the ~~apparatus, user apparatus comprises changing~~ a communication destination of the user apparatus ~~is changed to a specified device on the network.~~

8. (CURRENTLY AMENDED) A security management method according to Claim 7, wherein the specified device ~~sets the security level of the apparatus or provides a setting guide to the apparatus~~ controls updating the virus definition file of the user apparatus.

9. (CURRENTLY AMENDED) A recording medium recorded with a security management program for making a computer execute ~~step of:~~

detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

judging by comparing whether the security level of the user apparatus with reaches a predetermined security level; and

in the case of judging ~~that~~ the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus.

10. (CURRENTLY AMENDED) A recording medium recorded with a security management program according to Claim 9, ~~including a step of, in the~~ wherein in case of judging ~~that~~ the security level of the user apparatus reaches the predetermined security level, setting a range wider than the restriction range as the access permission range of the user apparatus.

11. (CURRENTLY AMENDED) A recording medium recorded with a security management program according to Claim 9, wherein in case ~~the step judges that~~ of judging the security level of the user apparatus does not reach the predetermined security level, ~~in the step of the~~ restricting of the access permission range of the ~~apparatus,~~ user apparatus comprises changing a communication destination of the user apparatus ~~is changed to~~ a specified device on the network.

12. (CURRENTLY AMENDED) A recording medium recorded with a security management program according to Claim 11, wherein the specified device controls updating the virus definition file of the user apparatus ~~sets the security level of the apparatus or provides a setting guide to the apparatus.~~

13. (CURRENTLY AMENDED) A security management system ~~configured comprising:~~

~~by connecting~~ a security management device, ~~an~~ apparatus for a user and a security setting guide device in communication via a network, ~~including:~~

wherein the security management device comprises:

a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus;

a judging unit judging ~~by comparing whether~~ the security level of the user apparatus ~~with~~ reaches a predetermined security level; and

an access control unit, in case the judging unit judges ~~that~~ the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user ~~of the~~ apparatus.

14. (CURRENTLY AMENDED) A security management system according to Claim 13, wherein the access control unit, in case the judging unit judges ~~that~~ the security level of the user apparatus does not reach the predetermined security level, connects ~~has~~ the user apparatus ~~connected~~ to the security setting guide device.

15. (NEW) A security management device including:
a controller
determining a security level of a user terminal upon a network access for the user terminal, based upon one or more of security information updating history of the user apparatus, port access information of the user terminal, or programs and/or scripts downloaded and/or executable at the user terminal, and
ensuring a predetermined security level on the network, according to the determined security level of the user terminal.

16. (NEW) The security management device of claim 15, wherein the security information comprises a virus definition file and the security information updating history of the user terminal comprises an access pattern to a security information server for updating the security information and/or an access history to the security information server for updating the security information.

17. (NEW) The security management device of claim 15, wherein the ensuring of the predetermined security level on the network comprises guiding the user terminal to meet the predetermined security level.

18. (NEW) The security management device of claim 15, wherein the ensuring of the predetermined security level on the network comprises if the security level of the user terminal does not reach the predetermined security level, restricting an access permission range on the network of the user terminal.